Current IETF Work on IP Mobility Support

Christian Vogt, chvogt@tm.uka.de
Institute of Telematics, University of Karlsruhe

March 2004

IETF's mobility-related working groups include MIP6, MIPSHOP, SEAMOBY, DNA, and NEMO. MULTI6 is not specifically concerned with mobility, but it discusses a similar set of problems that come along with allowing hosts to change their IP addresses. This overview summarizes the objectives of the MIP6, MIPSHOP, SEAMOBY, DNA, NEMO, and MULTI6 working groups. It illuminates relationships between different working groups and presents current activities. A synopsis is given in the second-to-last section. The tailing reference section gathers seminal working-group documents which may be of further interest to the reader.

MIP6 Working Group

The MIP6 working group was founded to enhance IPv6 with mobility supporting functionality. The working group's main document, "Mobility Support in Mobile IPv6" [1], specifies a protocol for binding a mobile node's identifier (a permanent IP address) to the mobile node's current locator (a more or less temporary IP address). [1] is in its 24th version, and the MIP6 community is becoming impatient in getting it accepted as an international standard. As matters stand, [1] is currently in the RFC editor's queue, waiting for publication as a proposed standard.

While the home agent plays a fundamental role in data relay in Mobile IPv4, Mobile IPv6 encourages two communicating parties to use the direct routing path for efficiency reasons. Using the direct routing path is called "Route Optimization" in [1]. Along with Route Optimization comes the fundamental issue of authentication between two communicating parties which do not know each other in advance. In most scenarios, neither is there a pre-shared secret between the two, nor does the MIP6 community want to depend on a not-yet-existing global public-key infrastructure. Mobile IPv6's solution is a protocol called "Return Routability", an approach that applies non-cryptographic, or "loose", authentication. Return Routability has been heavily debated, and many people feel that it fails to provide the security necessary for a wide employment of Mobile IPv6. On the other hand, there is currently no alternative to Return Routability that could make a difference. Cryptographically Generated Addresses [2] could be an excellent replacement for Return Routability, but the technique is patented by a group around Microsoft.

Apart from security deficits, many people think that Return Routability is too slow for applications that require fast handovers. Return Routability takes at least two round-trip times between two communicating parties. Three proposals have been presented at the 59th IETF summit which define an optional optimization for improved efficiency. With "Early Binding Updates for Mobile IPv6" [3] signaling can be moved off the critical path. This reduces the latency to one round-trip time between the communicating parties. "Optimizing Mobile IPv6 (OMIPv6)" [4] uses Return Routability to compute a secret key shared between the communicating parties. This key, once established, is used to authenticate signaling, thereby reducing latency to one round-trip time as well. "Preconfigured Binding

Management Keys for Mobile IPv6" [5] suggest using pre-shared secrets whenever two communicating parties have a permanent trust relationship.

MIPSHOP Working Group

The MIPSHOP working group was constituted at the 57th IETF meeting in July 2003 to handle protocols for localized mobility support. Prior to the formation of MIPSHOP, localized mobility support was considered part of the MOBILEIP working group's agenda, MIP6's predecessor. It was found that efforts on localized mobility support should better be outsourced to a separate working group. The MIPSHOP working group develops a hierarchical version of Mobile IPv6, "Hierarchical Mobile IPv6 mobility management (HMIPv6)" [6]. MIPSHOP works on "Fast Handovers for Mobile IPv6" (FMIPv6) [7], a protocol for enhanced handover performance between access routers within the same administrative domain.

HMIPv6 introduces a new architectural entity in the access network known as the Mobility Anchor Point. The Mobility Anchor Point serves as a local home agent for a mobile node. Downstream packets, and typically upstream packets as well, are tunneled between the mobile node and the Mobility Anchor Point. The mobile node maintains two care-of addresses. One is from the Mobility Anchor Point's sub-network, another is from its own subnet. The mobile node registers the former care-of address with its home agent and correspondent nodes. This care-of address does not change when the mobile node chooses to attach to a different access router within the domain of the same Mobility Anchor Point.

The idea of a hierarchical mobility management was taken from the Mobile IPv4 counterpart, "Mobile IPv4 Regional Registration" [8], developed earlier in the MOBILEIP working group. While HMIPv6's Mobility Anchor Point has Home Agent functionality, Regional Registration introduces a second hierarchy of Foreign Agents. The concept remains the same, though: A mobile node maintains two care-of addresses, a local one, which changes on every handover, and a regional one, which usually stays the same during movement.

FMIPv6 is a package with three components: a support protocol for finding a feasible new access router, a support protocol for IP-address configuration, and a support protocol for efficient data forwarding during handover. With FMIPv6, a mobile node can determine its next access router without having to connect to it. Instead, FMIPv6 lets the mobile node solicit the relevant information from its current access router. FMIPv6 defines a signaling protocol between the current and the new access router for IP-address configuration. This signaling protocol allows the mobile node to configure a new IP address before it moves to the sub-network where the new IP address is to be used. Moreover, FMIPv6 installs a tunnel between the old and the new access router such that packets, which are in flight to the mobile node's old access router, can be forwarded to the mobile node's new point of network attachment. The applicability of FMIPv6 in IEEE-802.11 networks [9] is an important item on the MIPSHOP working group's agenda.

A similar optimization, "Low Latency Handoffs in Mobile IPv4" [10], is has been developed for Mobile IPv4. Low Latency Handoffs leverage the Foreign Agent functionality available in the visited access network. Low Latency Handoffs define an Inter-Foreign-Agent protocol to allow a mobile node to register with its Home Agent a new Foreign Agent's care-of address through its current Foreign Agent. No Foreign Agent is available in FMIPv6. Therefore, due to security concerns, the mobile node can only register a new care-of address from the new link.

MIPSHOP maintains a document on requirements and goals for localized mobility management [11]. The document emphasizes efficiency with respect to latency and signaling overhead.

SEAMOBY Working Group

A mobile node's process of switching access routers can be smoothened by transferring state information pertaining to the mobile node from the old access router to the new one. The AAA context, header-compression information, and quality-of-service attributes are examples of state information which should follow, or lead the way for, a mobile node during movement. Moreover, a mobile node may be able to better prepare a handover through a pro-active discovery of alternative access routers. The SEAMOBY working group was founded to define protocols for both purposes. It has emphasized recent efforts on the Candidate Access Router Discovery protocol (CARD) [12] and the Context Transfer Protocol (CTP) [13].

A mobile node can use CARD to identify potential access routers. CARD allows a mobile node to retrieve an access router's administration and to determine whether it can authenticate with the router. Moreover, CARD allows the mobile node to solicit an access router's capabilities in order to find out whether these are appropriate for the application, or set of applications, currently running on the mobile node. Wireless network attachment should be characterized by a robust radio signal.

When a mobile node decides to change its point of network attachment, CTP helps to move the mobile node's current context from the old access router to the new one. The context may include header-compression data, authentication credentials, and accounting records. CTP is extensible in that it allows for the transferal of arbitrary context.

Both CARD and CTP are close to be finished. They will probably become experimental RFCs soon. The SEAMOBY working group maintains a document on mobility-related terminology [14]. This document is considered a dictionary for other working groups in this area as well.

DNA Working Group

Given a handover at the underlying link layer, a mobile node needs to determine whether this lower-layer handover has brought along attachment to a new IP network. Detection of network-attachment changes can significantly contribute to a handover's overall latency. Preferably, this detection should be precise, fast, and with limited as well as link-local signaling. Today's solutions, however, can only provide any two of these properties [15]. The primary goal of the newly established DNA working group is to explore mechanisms that can provide all three properties at the same time [16].

When a mobile node recognizes that it has switched to a new IP network, the mobile node needs to invoke network-layer re-configuration procedures in order to retain the ability to send and receive IP packets. This typically includes Router Discovery and IP-address configuration. A second goal of the DNA working group is to streamline this re-configuration process.

In a first step, the DNA working group will publish an RFC on best current practices for network-attachment detection and handling. This document will be based on existing standards like Router Discovery and Neighbor Unreachability Detection for movement detection as well as Stateless Address Configuration for network-layer re-configuration. An important step towards anticipated and more robust handovers is the provision of link-layer triggers. It is envisioned that a basic set of link-layer triggers will be considered in the first RFC.

In a second step, the DNA working group will analyze more sophisticated techniques for movement detection and network-layer re-configuration. These are likely to require a wider set of link-layer triggers. For instance, if a mobile node was informed, by its link layer, about a fading radio signal ahead of time, the mobile node could aggressively look for alternative points of network attachment. A

set of advanced link-layer triggers – spanning the realm of IEEE-802.3, IEEE-803.11, IEEE-802.15, and IEEE-802.16 networks – is currently being defined by the IEEE 802.21 working group. DNA and IEEE 802.21 are likely to cooperate closely.

Beyond the ability to identify a new access router, a mobile node should know whether or not it can authenticate with the access router before it attempts to attach to it. The mobile node should also be warned if firewalls behind a potential new access router prevent the continuation of ongoing communications. There may be difficulties due to VPN connections, for example. The DNA working group will attend to this in the future, but no specific proposals exist at this time.

NEMO Working Group

Mobile IP allows a mobile node to switch between access routers in a manner transparent to an application. Beyond the wireless link, the network infrastructure is expected to be static. The NEMO working group explores scenarios in which a router, too, can move. The "Network Mobility (NEMO) Basic Support Protocol" [17] defines a basic mechanism for network mobility based on the existing Mobile IPv6 standard. It uses bi-directional tunneling between a mobile router and its home agent. Packets for a node within a mobile network are sent to the mobile router's home agent. The home agent encapsulates these packets and forwards them to the mobile router. The mobile router, in turn, decapsulates the packets and forwards them on to final recipient's interface. The opposite procedure is used for packets coming from a node within the mobile network addressed to some correspondent outside.

In a future step, the NEMO working group will analyze the applicability of route optimization for optimized packet relay between a mobile router and a set of correspondent nodes. The working group will investigate into potential threats that come along with route optimization. Further optimization may be doable by making nodes aware of network mobility.

MULTI6 Working Group

There are reasons as to why a site should be connected to the public Internet by more than one ISP [18]. One such reason is fault tolerance: If the connection through one ISP fails, Internet access can be upheld through a different ISP. Another reason is load balancing: A site may choose to spread its workload over multiple ISPs in a way depending on both its own load as well as the ISPs' load.

With IPv4, multi-homed sites are usually allocated provider-independent subnet prefixes. Somewhere in the Internet's default-free zone, a router needs to make a decision which path to use for packets destined to a multi-homed site. Using a single, provider-independent subnet prefix for a multi-homed site saves address space, because one (provider-independent) IP address per host is enough. This is why this approach is favorable for IPv4. On the other hand, provider-independent subnet prefixes cause routing tables in the default-free zone to grow, because they cannot be aggregated with any ISP's address space. Due to the large number of IPv6 addresses, this approach is bound not to scale in an IPv6 Internet. With IPv6, multi-homed hosts will be assigned a separate subnet prefix from each ISP. These prefixes can be aggregated in the default-free zone in the usual way. The question here is how a host can determine which IP address to use for packets addressed to a multi-homed peer.

The MULTI6 working group seeks to find a solution to the multi-homing problem in IPv6. One approach currently under discussion [19] is such that DNS holds, for each multi-homed host, the set of that host's IPv6 addresses. This address set is mapped to by a fully-qualified domain name uniquely

identifying the host. Through DNS, a multi-homed host therefore remains reachable for any host seeking contact. A multi-homed host uses as its packets' source addresses the IPv6 address it prefers to be reached through. The source address can be rewritten by routers.

The set of a multi-homed host's addresses may change due to prefix renumbering. Such changes are assumed to occur infrequently enough to facilitate use of DNS in spite of its slow update times. In contrast, DNS updates are not an option for mobile nodes, because those are expected to change their (care-of) addresses much more frequently. Mobile IP's solution to fast-changing addresses is the home-agent concept: Each mobile node is assigned an almost-permanent home address, which can be bound to a new care-of address relatively fast.

Research on multi-homing is not directly related to mobility. It turns out, however, that multi-homing introduces new potential threats similar to those considered in the mobility context. These threats are largely described as re-direction attacks. Re-direction happens when a malicious node causes packets to be sent to a host that does not expect these packets. Re-direction can result in the recipient's denial of service. It may occur when there is insufficient validation that a host is the legitimate owner of the IP address that it uses.

Synopsis

The following table summarizes the objectives and current activities of IETF's MIP6, MIPSHOP, SEAMOBY, DNA, NEMO, and MULTI6 working groups.

	Objectives	Current Activities
MIP6	Mobility support for IPv6.	Publish Mobile IPv6 as an RFC.
MIPSHOP	Efficient mobility management in administrative access-network domains.	Publish HMIPv6 and FMIPv6 as RFCs.
SEAMOBY	State and context transfer between network entities at the edge of the Internet.	Publish CARD and CTP as experimental RFCs.
DNA	Efficient detection of network-attachment changes.	Publish an RFC on best current practices in network-attachment detection.
NEMO	Automatic network attachment for mobile routers.	Use Mobile IPv6 to connect a mobile router to the router's home agent.
MULTI6	Site multi-homing in an IPv6-enabled Internet.	Assign multiple IPv6 addresses to a multi-homed host. Use DNS for mapping a host's identity to the set of its addresses.

References

[1] David Johnson, Charles Perkins, Jari Arkko: Mobility Support in Mobile IPv6, draft-ietf-mobileip-ipv6-24.txt, June 2003.

[2] Greg O'Shea, Michael Roe: Child-proof Authentication for MIPv6 (CAM), Microsoft Research Ltd., April 2001.

[3] C. Vogt, R. Bless, M. Doll, T. Küfner: Early Binding Updates for Mobile IPv6, draft-vogt-mip6-early-binding-updates-00.txt, February 2004.

[4] W. Haddad, F. Dupont, L. Madour, S. Krishnan, S. Park: Optimizing Mobile IPv6 (OMIPv6), draft-haddad-mipv6-omipv6-01.txt, February 2004.

[5] Charles Perkins: Preconfigured Binding Management Keys for Mobile IPv6, draft-perkins-mobileip-precfgKbm-00.txt, April 2004.

[6] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier: Hierarchical Mobile IPv6 mobility management (HMIPv6), draft-ietf-mipshop-hmipv6-01.txt, February 2004.

[7] Rajeev Koodli: Fast Handovers for Mobile IPv6, draft-ietf-mipshop-fast-mipv6-01.txt, January 2004.

[8] Eva Gustafsson, Annika Jonsson, Charles Perkins: Mobile IPv4 Regional Registration, draft-ietf-mobileip-reg-tunnel-08.txt, November 2003.

[9] Pete McCann: Mobile IPv6 Fast Handovers for 802.11 Networks, draft-ietf-mipshop-80211fh-00.txt, February 2004.

[10] Karim El Malki: Low Latency Handoffs in Mobile IPv4, draft-ietf-mobileip-lowlatency-handoffs-v4-08.txt, January 2004.

[11] Carl Williams: Localized Mobility Management Goals, draft-ietf-mipshop-lmm-requirements-02.txt, February 2003.

[12] M. Liebsch, A. Singh, H. Chaskar, D. Funato, E. Shim: Candidate Access Router Discovery, draft-ietf-seamoby-card-protocol-06.txt, December 2003.

[13] J. Loughney, M. Nakhjiri, C. Perkins, R. Koodli: Context Transfer Protocol, draft-ietf-seamoby-ctp-08.txt, January 2004.

[14] J. Manner, M. Kojo: Mobility Related Terminology, draft-ietf-seamoby-mobility-terminology-06.txt, February 2004.

[15] Y. Han, J. Choi, H. Jang, S. Madanapalli, O. Rao, Wable R U: Current Schemes for Movement Detection, Samsung, February 2004.

[16] JinHyeock Choi, Gregory Daley: Detecting Network Attachment in IPv6 Goals, draft-jinchoi-dna-goals-00.txt, February 2004.

[17] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert: Network Mobility (NEMO) Basic Support Protocol, draft-ietf-nemo-basic-support-02.txt, December 2003. ---

[18] Joe Abley, Benjamin Black, Vijay Gill: Goals for IPv6 Site-Multihoming Architectures, RFC 3582, August 2003.

[19] Erik Nordmark: Multihoming without IP Identifiers, draft-nordmark-multi6-noid-01.txt, October 2003.